

# Signed ECH Configs

Nick Sullivan, Dennis Jackson, Alessandro Ghedini

# Outline

- Goal
- Mechanism
- Why

# Goal: Make ECH easier to deploy

## With ECH:

1. Choose an Outer SNI
2. Register the domain (\$\$\$)
3. Get a TLS Cert
4. Provision your server
5. Update your ECHConfigs

# Goal: Make ECH easier to deploy

## With ECH:

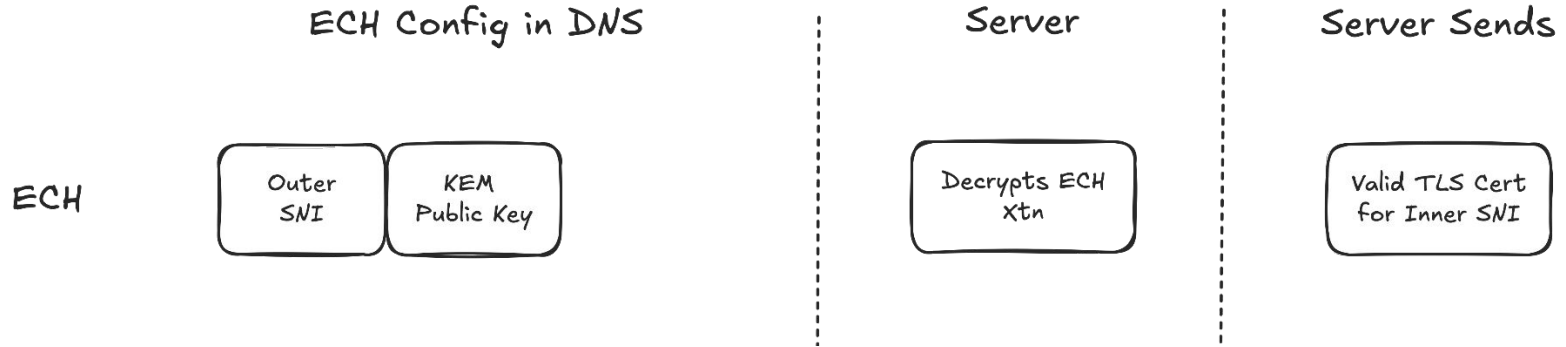
1. Choose an Outer SNI
2. Register the domain (\$\$\$)
3. Get a TLS Cert
4. Provision your server
5. Update your ECHConfigs

## With Signed ECH:

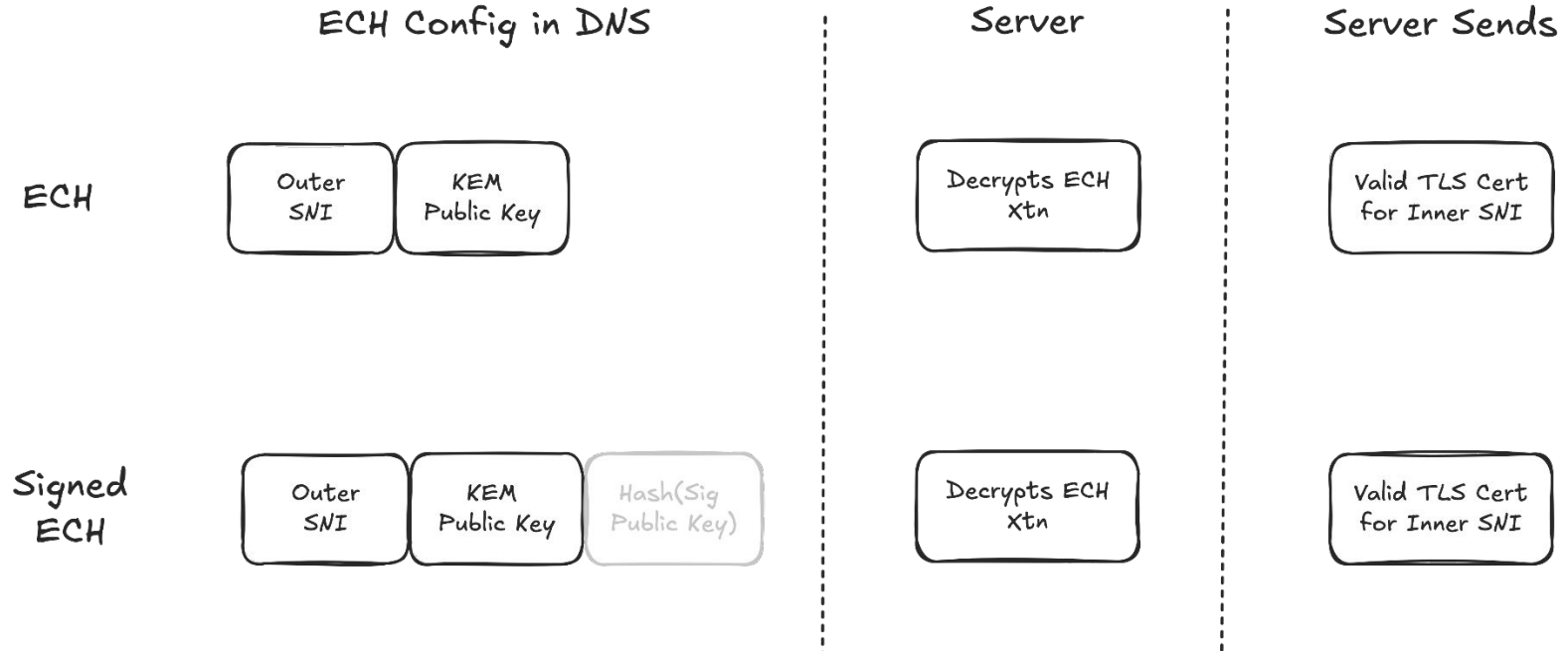
1. Choose an Outer SNI
2. Update your ECHConfigs

# How: Happy Path

# How: Happy Path

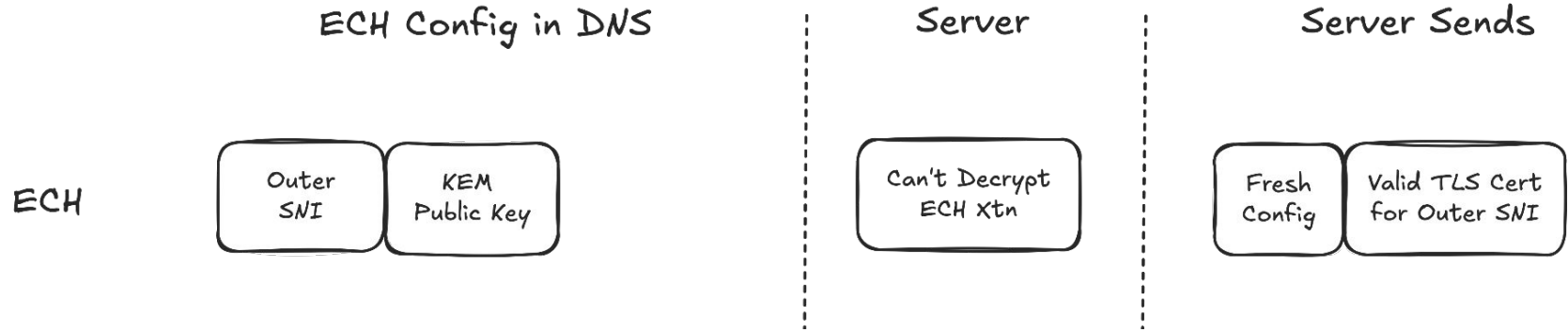


# How: Happy Path

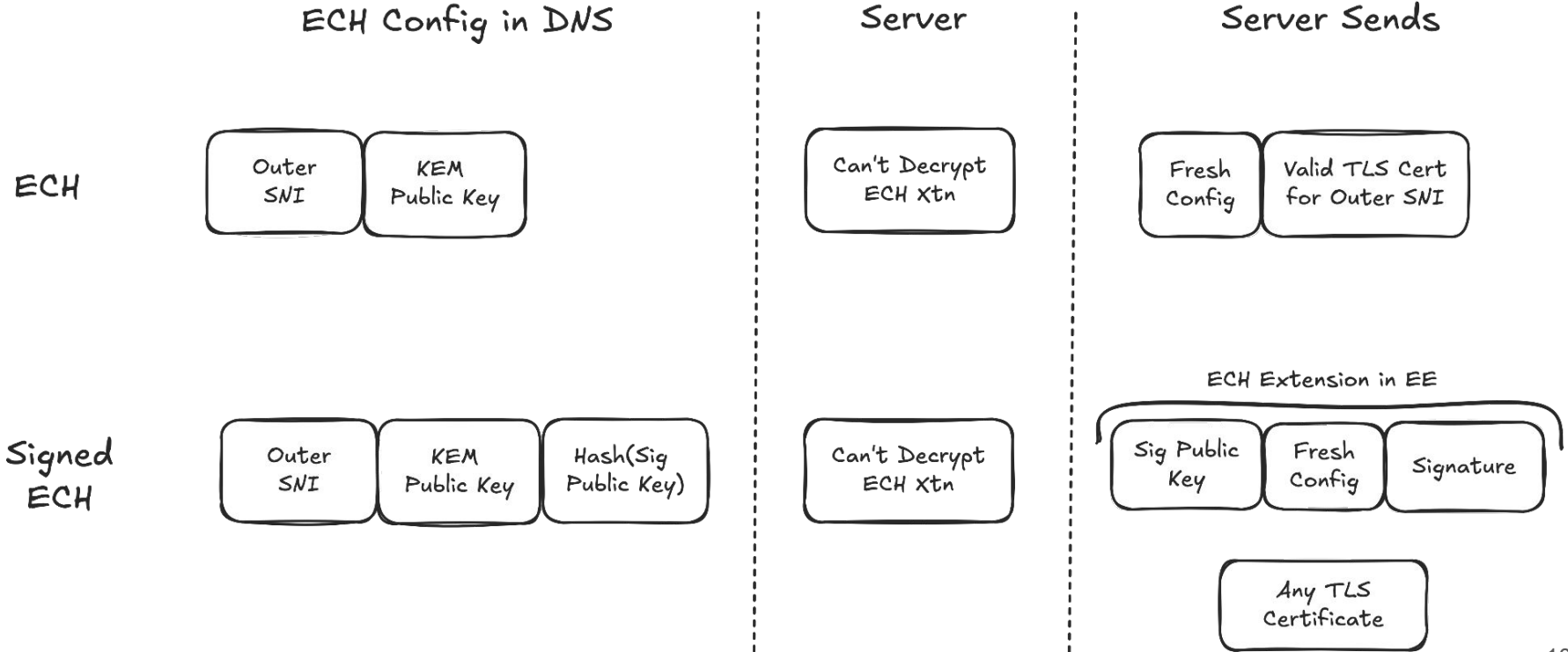


# How: Fallback

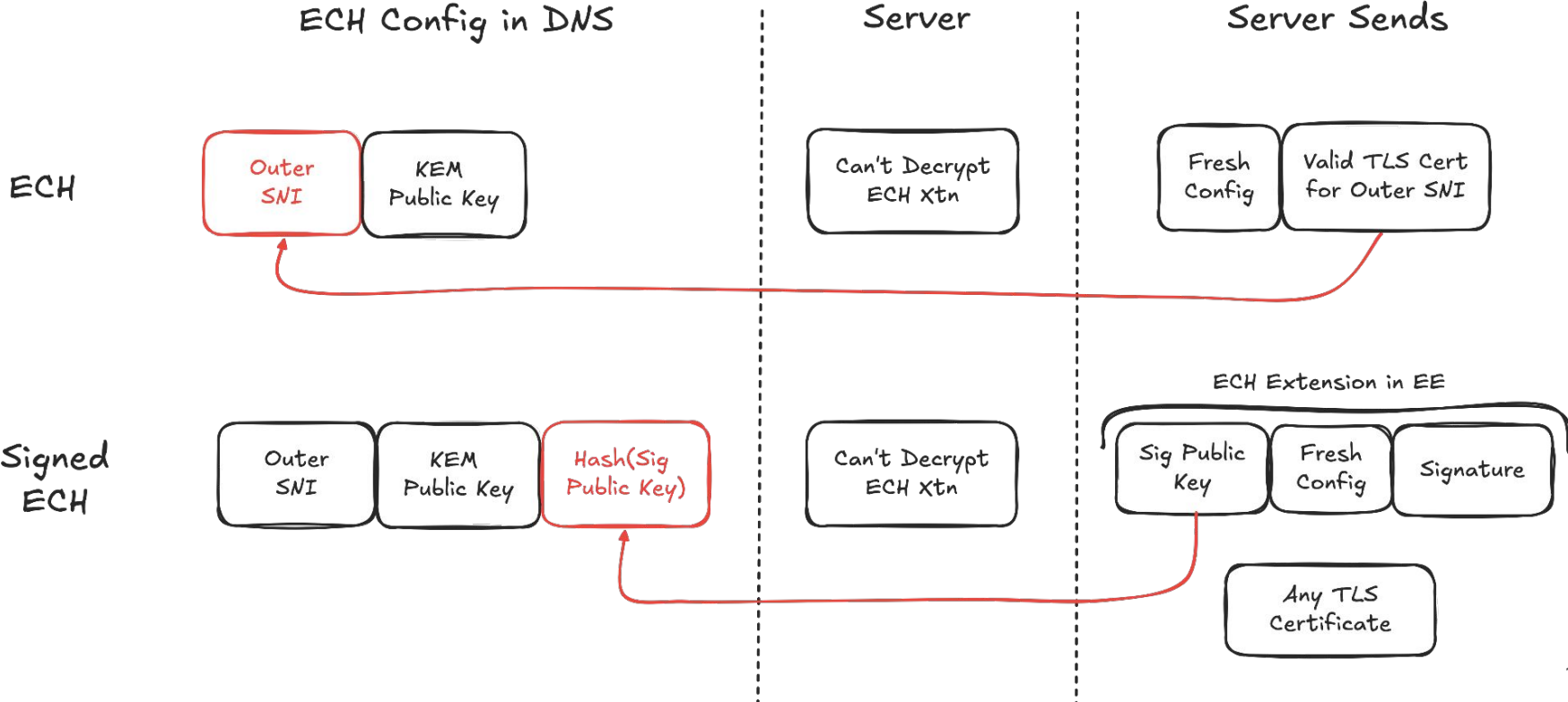
# How: Fallback



# How: Fallback



# How: Fallback



# Why?

Reducing information flow:

1. Set field to a fixed string (ECH)
2. Set field to a random string (Signed ECH)

Every connection can use a random SNI.

This does not require coordination or collaboration between sites in an anonymity set.

This is less fragile in the presence of middleboxes

# Easier to deploy

1. A webserver can enable Signed ECH by default. No need for external configuration or to ask the user to register a cover domain name.
  
2. CDN Customers do not need to fate-share.
  - a. Do you want to pool your connections with others on one easily blockable domain?
    - i. Uh, no?
  - b. Do you want to use random non-shared SNIs to improve customer privacy?
    - i. Maybe, Yes?

# Less Fragile

ECH:

If SNI == '[cdn-ech.com](https://cdn-ech.com)' => DROP PACKET;

SNI blocklists are pervasive.



# Less Fragile

## ECH:

If SNI == '[cdn-ech.com](https://cdn-ech.com)' => DROP PACKET;

SNI blocklists are pervasive.

## Signed ECH:

1. Active probing
2. Internet-wide scans to maintain domain-ip mappings

Requires active and ongoing infrastructure investment.



# Now and Next

- Nick has developed some interop code (Rust / Go / C)
  - <https://github.com/grittygrease/ech-auth-interop>
  
- (At least) one more round of trimming the draft
  - Thank you for the feedback on the mailing list!

# Details

- Key Rotation:
  - DNS ECHConfig has a list of public key hashes. Any of them are suitable.
  - Add new public key before retiring old public key.
  - Don't need to rotate often - no perfect forward secrecy compromise
  
- Replay Attacks
  - Fallback signature includes a not\_after field.
  - Prevents attacker trying to downgrade other users by serving stale fallback information.